APHIS PRIMARY DATA CENTER ACCESS

1. PURPOSE

This Directive establishes APHIS policy and procedures for management and control of physical access to the APHIS Primary Data Centers.

2. REFERENCES

a. National Institute of Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems.

b. Federal Information Systems Controls Audit Manual (FISCAM), Volume 1; Financial Statement Audits.

3. SCOPE

This Directive applies to all persons who need access to APHIS Primary Data Centers including APHIS employees, contractors, and building support services personnel.

4. DEFINITIONS

a. Primary Data Center (Computer Room). An APHIS controlled room containing sensitive or critical IT equipment and designated by the APHIS Chief Information Officer (CIO) as a Primary Data Center, also referred to as Computer Room in this Directive. These facilities are listed in Attachment 2.

b. Lenel OnGuard ("Lenel"). The security system implemented by APHIS for building physical access control, and ID credential issuance and management.

c. Data Center Access Report. A report generated by Lenel, listing persons who have gained access to a building area during a specified time period, via authorized (Lenel) badge.

d. Data Center Approved Personnel Access List. A report generated by Lenel, listing persons who are authorized for access to a specified building area.

e. Recertification. The process for confirming that an individual's access privileges to an APHIS Primary Data Center have been properly authorized and are still required.

5. POLICY

Secure management of access to its Primary Data Centers is vital to protecting APHIS computer systems and information. Section 2.a. and b. provide recommended security controls to accomplish this objective. This Directive establishes APHIS policy and processes for the implementation of these security controls, as follows:

a. APHIS Form 514, APHIS Data Center Access Control Form (Attachment 1), will be used to request access to APHIS Primary Data Centers. This form will be used as a supplement to the existing Facility Access Request form.

b. The Employee Services Division (ESD) will perform all badge issuance and perform all activation/de-activation of badge access privileges.

c. All access granted to the Primary Data Centers must be coordinated with the APHIS Human Resources Security Officer to validate proper security clearance.

d. Data Center Access Reports will be reviewed weekly for inappropriate access.

e. Data Center Approved Personnel Access Lists will be reviewed monthly to ensure that all persons on the Lists have been properly authorized for access per the terms of this Directive.

f. Anyone who has not exercised his/her access privileges to an APHIS Primary Data Center in 90 days will be removed from the Data Center Approved Personnel Access List.

g. Access privileges will be removed within 30 days of:

(1) Employee termination (for APHIS employees);

(2) Cessation of work for which access was required (for contractors and all others).

h. All Primary Data Center access privileges will be recertified at least annually.

i. Guests will be escorted at all times while in a Primary Data Center, by a person with current Primary Data Center access privileges.

j. Guests must sign in and out of the Primary Data Center Visitor Log Book for every visit.

6. RESPONSIBILITIES

a. The Chief Information Officer will:

(1) Approve and ensure implementation of this Directive.

(2) Approve any modifications to this Directive.

b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:

(1) Disseminate this Directive to their respective staffs.

(2) Ensure that the terms of this Directive are followed within their Program Units, and that appropriate procedures are developed and implemented to support the processes mandated by this Directive.

(3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.

c. APHIS Supervisors and Contracting Officer Technical Representatives (COTRs) for APHIS contractors will:

(1) Ensure that APHIS Form 514 is completed and forwarded to the appropriate Computer Room Manager.

(2) Authorize requests for access to APHIS Primary Data Centers by signing APHIS Form 514 and giving, mailing, or e-mailing it to the Computer Room Manager. (If the form is e-mailed, it must be sent from the supervisor's/COTR's e-mail account).

d. The MRPBS, ITD, Information Security Officer will:

(1) Maintain this Directive, including receiving requests for, and executing modifications in response to change requests and/or new requirements.

(2) Review, approve, and sign all reports and reviews generated under the terms of this Directive.

(3) Perform an annual review of Primary Data Center access procedures to ensure that the terms of this Directive are followed. He/she will:

(a) Inspect documentation on file to ensure that records are maintained in compliance with the terms of this Directive.

(b) Ensure that deviations identified are corrected within 30 days.

(c) Document, sign, and file a report summarizing the steps, findings, and corrective actions taken during the review.

(d) Retain annual review reports for a period of 5 years. These records will be maintained and disposed of by calendar year (no incremental disposal), to ensure availability for audit purposes.

e. The MRPBS, Employee Services Division (ESD) will:

(1) Manage the issuance and revocation of all badges for Primary Data Centers.

(2) Manage the activation and de-activation of all badge access for Primary Data Centers.

f. MRPBS, ITD, Computer Room Managers will:

(1) Manage access to APHIS Primary Data Centers in conformance with the terms of this Directive.

(2) Prior to granting access, ensure that the employee or contractor has:

(a) A verifiable need to access a resource on the premise.

(b) A completed and approved APHIS Data Center Access Control Form.

(c) The appropriate level of security clearance, to be verified with the APHIS Human Resources Security Officer.

(3) Weekly, obtain a Data Center Access Report. He/she will:

(a) Review it for inappropriate access, and take appropriate corrective action.

(b) Notate the report to indicate review findings and actions taken.

(c) Retain notated reports for a period of one year. These records will be maintained and disposed of by calendar year (no incremental disposal), to ensure availability for audit purposes.

(4) Monthly, obtain a Data Center Approved Personnel Access List. He/she will:

(a) Review it to ensure that an appropriately approved APHIS Data Center Access Control Form is on file for each person on the List, or take appropriate action to revoke access.

(b) Review it to ensure that each person on the List has exercised his/her access privileges within the last 90 days, or take appropriate action to revoke access.

(c) Notate the list to indicate review findings and corrective actions taken.

(d) Retain notated lists for a period of 1 year. These records will be maintained and disposed of by calendar year (no incremental disposal), to ensure availability for audit purposes.

(5) Annually, perform a Primary Data Center Access Recertification, as follows:

(a) Obtain a Data Center Approved Personnel Access List for the Primary Data Center for which he/she is responsible.

(b) For each individual on the access list, contact the appropriate supervisor or COTR and obtain written confirmation that the individual's access is still required, or take action to revoke the individual's access.

(c) Prepare a report summarizing the Annual Recertification steps, findings, and corrective actions taken.

(d) Submit an Annual Recertification Report to the Manager, MRPBS, ITD, Information Security Office, for review and signature, to verify the results of the recertification and that appropriate corrective actions were taken.

(e) Retain Annual Recertification Reports for a period of 5 years. These records will be maintained and disposed of by calendar year (no incremental disposal), to ensure availability for audit purposes.

f. APHIS employees will use the procedures outlined in this Directive when requesting access to APHIS Primary Data Centers.

7. INQUIRIES

a. Questions concerning the information and processes described in this Directive should be directed to the Manager, MRPBS, ITD, Information Security Office.

b. This Directive can be accessed at ***www.aphis.usda.gov/library***

/s/
Gregory L. Parham
APHIS Chief Information Officer

Attachments

Attachment 1

UNITED STATES DEPARTMENT OF AGRICULTURE
ANIMAL AND PLANT HEALTH INSPECTION SERVICE
MARKETING AND REGULATORY PROGRAMS BUSINESS SERVICES
INFORMATION TECHNOLOGY DIVISION

APHIS DATA CENTER ACCESS CONTROL FORM

Blocks 1 through 10 to be completed by Requestor

1. NAME

Last Name: **First Name:** **Middle Initial:**

2. DATE OF REQUEST

3. PHONE NUMBER *(Including area code)*

4. EMAIL ADDRESS

5. EMPLOYER *(Choose only one)*

☐ **APHIS**
☐ **CONTRACTOR**
☐ **OTHER**

6. TYPE OF REQUESTED ACCESS *(Choose only one)*

☐ **PERMANENT**
☐ **TEMPORARY/EMERGENCY** *(Must complete Block 10)*

7. DATA CENTER(S) TO WHICH ACCESS IS REQUESTED *(Include location names)*

8. ACTION REQUESTED *(Choose only one)*

☐ **Establish new access account**
☐ **Terminate access account**
☐ **Modify access account** *(use Block 9 to specify instructions)*

9. INSTRUCTIONS FOR ACCESS MODIFICATION *(if applicable)*

10. DURATION / HOURS OF REQUESTED ACCESS *(If requesting temporary/emergency access, must specify termination date and hours of requested access. For example, business hours, evenings, weekends, etc.)*

Blocks 11 through 15 to be completed by Requestor if Requestor is not an APHIS employee

11. NAME AND ADDRESS OF EMPLOYER *(Company, or Federal/State/Local Agency)*

12. SUPERVISOR *(Name, Title, Phone Number)*

13. CONTRACT NUMBER *(if applicable)*

14. APHIS POINT OF CONTACT *(For example, Contracting Officer Representative)*

15. REASON FOR ACCESS *(Please describe the nature of the tasks being performed by the Requestor)*

Block 16 to be completed by Supervisor (if Requestor is an APHIS employee), APHIS Contracting Officer Technical Representative (if Requestor is a contractor), or authorizing APHIS Point of Contact (for all others)

16. APHIS AUTHORIZING OFFICIAL

(Signed) _____ (Date)_____

Print name and title:

Blocks 17 and 18 to be completed by APHIS Computer Room Manager

17. COMPUTER ROOM MANAGER

(Signed) _____ (Date)_____

Print name and title:

18. ACTION TAKEN

Instructions for completing APHIS Data Center Access Control Form:

1. APHIS Supervisors and Contracting Officer Technical Representatives (COTRs) for APHIS contractors will complete this form and forward it to APHIS Computer Room Managers for the following events:

    a. Data Center access permission - form will be submitted within 14 calendar days of access need.

    b. Termination – form will be submitted within 14 calendar days following employee or contractor termination, or cessation of work for which access was required.

2. If multiple Data Centers are listed in Block 7, Requestor will send a copy of the completed form to each Computer Room Manager.

Attachment 2

APHIS Primary Data Centers

Location	Room Number	Room Name
Riverdale, MD	2C02	Computer Room
Fort Collins, CO	1E25 1E26	Computer Room Network Control Center (interior room inside 1E25)
Minneapolis, MN	6th Floor (no room number)	Computer Room
Raleigh, NC	225	Computer Room